

IFW

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re patent application of

Applicant: **Ramarathnam Venkatesan et al.**  
Serial No.: **10/803,108**  
Filed: **March 17, 2004**  
For: **Unimodular Matrix-based Message Authentication Codes (MAC)**  
Art Unit: **2186**  
Examiner: **Unknown**

**INFORMATION DISCLOSURE STATEMENT**

Assistant Commissioner for Patents  
Alexandria, Virginia 22313-1450

Sir:

1. Pursuant to 37 C.F.R. 1.97 and 1.98, and in compliance with 37 C.F.R. 1.56, the Office's attention is directed to the patents, publications and other information listed on the attached PTO-1449. A copy of each listed document is enclosed except for: (a) pending applications or (b) those previously cited or submitted to the Office in the following application(s) upon which this application relies for an earlier filing date under 35 U.S.C. 120; or (c) U.S. Patent(s) and published applications(s) since the subject application was filed after June 30, 2003.

Serial No.: \_\_\_\_\_  
Filing Date: \_\_\_\_\_

Regarding any document, publication or other information for which a date is not given on the attached PTO-1449, Applicant(s) believe(s) the same may qualify as "prior" art to this application and should be treated accordingly, although Applicant(s) reserve(s) the right to contest the prior art status of any document, publication or information, should issue arise.

2. Regarding each listed document that is not in the English language, an English-language translation accompanies this Statement as indicated on the attached PTO-1449 or a concise explanation of the relevance of the document is set forth in the following document(s):

(a) \_\_\_ Copy of each English language version of a search report indicating the degree of relevance found by the foreign office of each document being submitted from the search report.

(b) \_\_\_ Attachment entitled "Concise Explanation of Relevance of Non-English Language Documents".

3. Pursuant to 37 C.F.R. 1.97(b) this Statement is being filed (one must be checked):

(a) **X** Within 3 months of the filing date or date of entry into the National Stage.

(b) \_\_\_ Before the mailing date of a first Office Action on the merits. If this Statement is not filed before the mailing date of a first Office Action on the merits, the required certification is given below or, in the absence thereof, the Office is authorized to charge the required fee set forth in 37 C.F.R. 1.17(p) to Deposit Account No. 50-1063 for consideration of this Statement.

(c) \_\_\_ After the period set forth in 37 C.F.R. 1.97(b) but before the mailing date of either a final action or a notice of allowance.

(1) \_\_\_ The required certification is given below, or

(2) \_\_\_ Enclosed is a check covering the fee set forth in 37 C.F.R. 1.17(p) for consideration of this Statement, or

(3) \_\_\_ Charge the fee set forth in 37 C.F.R. 1.17(p) to Deposit Account No. 50-1063.

(d) \_\_\_ After the mailing date of either a final action or a notice of allowance, but before payment of the issue fee. Petition hereby is made for consideration of this Statement and the required certification is indicated below.

(1) \_\_\_ Enclosed is a check covering the fee set forth in 37 C.F.R. 1.17(i)(1), or

(2) \_\_\_ Charge the fee set forth in 37 C.F.R. 1.17(i)(1) to Deposit Account No. 50-1063.

4. Certification (if applicable)

(a) \_\_\_ The undersigned hereby certifies that each item of information contained in this Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than 3 months prior to the filing of this Statement.

(b) \_\_\_ The undersigned hereby certifies that no item of information contained in this Statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the undersigned's knowledge after making reasonable inquiry, was known to any individual designated in 37 C.F.R. 1.56(c) more than 3 months prior to the filing of this Statement.

5. The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1063.

Respectfully Submitted,

By Jeffrey R. Sadlowski  
Jeffrey R. Sadlowski  
Reg. No. 47,914

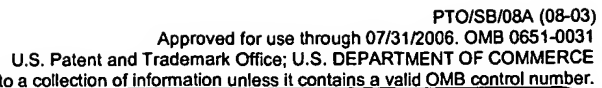
24<sup>TH</sup> Floor, National City Center  
1900 East 9<sup>th</sup> Street  
Cleveland, Ohio 44114  
(216) 696-8730

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence (along with any paper referenced as being attached or enclosed) is being deposited on the below date with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Assistant Commissioner for Patents, Alexandria, Virginia 22313-1450.

Date: 6-16-2004

Jeffrey R. Sadlowski  
Jeffrey R. Sadlowski



Substitute for form 1449/PTO

**(Use as many sheets as necessary)**

Sheet	1	of	2
-------	---	----	---

**Complete if Known**

Application Number	10/803,108
Filing Date	March 17, 2004
First Named Inventor	Ramarathnam Venkatesan
Art Unit	2186
Examiner Name	Unknown
Attorney Docket Number	MS306485.1/MSFTP540US

## U. S. PATENT DOCUMENTS

## FOREIGN PATENT DOCUMENTS

**Examiner  
Signature**

Date  
Considered

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>2</sup> Applicant's unique citation designation number (optional). <sup>3</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>4</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>5</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>6</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>7</sup> Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)		<b>Complete if Known</b>			
		Application Number	10/803,108		
		Filing Date	March 17, 2004		
		First Named Inventor	Ramarathnam Venkatesan		
		Art Unit	2186		
		Examiner Name	Unknown		
Sheet	2	of	2	Attorney Docket Number	MS306485.1/MSFTP540US

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		M. BELLARE, R. CANETTI, H. KRAWCZYK. Keying hash functions for message authentication. In Advances in Cryptology - CRYPTO'96, vol. 1109 of Lecture Notes in Computer Science Springer-Verlag, pp. 1-15, 1996.	
		J. BLACK, S. HALEVI, H. KRAWCZYK, T. KROVETZ, and P. ROGAWAY. UMAC: Fast and Secure Message Authentication. Advances in Cryptology - CRYPTO '99. Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, pp. 216-233, 1999.	
		P. ROGAWAY. Bucket hashing and its applications to fast message authentication. Journal of Cryptology, Vol. 12 No. 2, 1999. 24 pages.	
		DANIEL J. BERNSTEIN. Floating-point Arithmetic and Message Authentication. Journal of Cryptography, March 2000. 20 pages.	
		UMAC Performance. <a href="http://www.cs.ucdavis.edu/~rogaway/umac/perf00.html">http://www.cs.ucdavis.edu/~rogaway/umac/perf00.html</a> . Last Updated on August 29, 2000.	
		UMAC Performance (More). <a href="http://www.cs.ucdavis.edu/~rogaway/umac/perfbis00.html">http://www.cs.ucdavis.edu/~rogaway/umac/perfbis00.html</a> . Last Updated on August 29, 2000.	
		UMAC Code. <a href="http://www.cs.ucdavis.edu/~rogaway/umac/code.html">http://www.cs.ucdavis.edu/~rogaway/umac/code.html</a> . Last Updated on August 7, 2000.	
		J. BLACK, S. HALEVI, H. KRAWCZYK, T. KROVETZ, P. ROGAWAY. Update on UMAC Message Authentication. May 2000. 1 page.	
		T. KROVETZ, J. BLACK, S. HALEVI, A. HEVIA, H. KRAWCZYK, and P. ROGAWAY. UMAC: Message Authentication Code using Universal Hashing. IPsec Working Draft, October 2000. <a href="http://www.cs.ucdavis.edu/~rogaway/umac/draft-krovetz-umac-01.txt">http://www.cs.ucdavis.edu/~rogaway/umac/draft-krovetz-umac-01.txt</a>	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.